

ADDENDUM RELATIF AU TRAITEMENT DES DONNÉES

1 GÉNÉRALITÉS

- 1.1 Le présent addendum relatif au traitement des données définit les conditions qui s'appliquent au traitement des données personnelles des clients par Keyloop dans le cadre de la fourniture des services. Il fait partie intégrante du contrat conclu entre Keyloop et le client.
- 1.2 Le Centre de confidentialité fournit des informations supplémentaires sur la manière dont Keyloop traite les données personnelles du client.

2 DÉFINITIONS ET INTERPRÉTATION

- 2.1 Tous les termes en majuscules dans le présent addendum relatif au traitement des données ont la signification qui leur est donnée dans le contrat, sauf indication contraire ci-dessous ou dans l'annexe 1 du présent addendum.
- 2.2 Les termes suivants ont la signification suivante dans le présent addendum relatif au traitement des données :

Contrat le contrat conclu entre le client et Keyloop pour la fourniture des services, comprenant la documentation ;

Les données personnelles du client désignent les données personnelles fournies par le client ou les

les sociétés affiliées du client à Keyloop, ou qui sont traitées par Keyloop pour le compte du client ou des sociétés affiliées du client, conformément au contrat ;

Détails du traitement des données les détails concernant le traitement des données personnelles du client par Keyloop, tels qu'indiqués dans le Centre de confidentialité ;

Autorité de protection des données désigne une autorité réglementaire, administrative, de contrôle ou

agence, organisme ou autorité gouvernementale ayant compétence sur les activités de traitement des données à caractère personnel envisagées dans le présent addendum sur le traitement des données ;

Législation sur la protection des données désigne toutes les lois applicables relatives au traitement des données à caractère personnel, en vigueur à tout moment, telles que (le cas échéant) :

(a) le RGPD de l'UE ;

(b) la loi britannique sur la protection des données ;

- (c) la loi allemande de 2018 sur la protection des données ;
- (d) la loi portugaise sur la protection des données comprenant la loi n° 58/2019 du 8 août et la loi n° 41/2004 du 18 août ;
- (e) la loi sur la protection des renseignements personnels et les documents électroniques (PIPEDA) et les lois provinciales essentiellement similaires ;
- (f) la loi fédérale sur la protection des données personnelles détenues par des entités privées au Mexique ;
- (g) la loi de 2012 sur la protection des données personnelles de Singapour ;
- (h) la loi sud-africaine de 2013 sur la protection des informations personnelles n° 4
- (i) le décret-loi fédéral n° 45/2001 sur la protection des données personnelles aux Émirats arabes unis ;
- (j) la loi fédérale suisse sur la protection des données ;
- (k) la loi sur la protection des données personnelles B.E. 2562 (A.D. 2019) et toute réglementation ou annonce relative à la protection des données personnelles émise en vertu de cette loi en Thaïlande ; et
- (l) toute autre loi et tout autre instrument réglementaire relatifs à ces réglementations, à la protection des données ou à la vie privée ;

Destinataire des données a la signification qui lui est donnée à la clause 7.1 ;

RGPD règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, connu sous le nom de règlement général sur la protection des données (UE) 2016/679 ;

Centre de confidentialité désigne le Keyloop « Privacy » disponible sur <https://www.keyloop.com/legal-documentation> ;

Sous-traitant tout sous-traitant tiers désigné par Keyloop, qui peut recevoir et/ou avoir accès aux données personnelles du client ;

Transfert désigne le transfert, l'accès ou le traitement des données personnelles du client à un destinataire des données ;

Loi britannique sur la protection des données comprend :

- (a) le RGPD de l'UE, qui fait partie intégrante du droit anglais, gallois, écossais et nord-irlandais en vertu de l'article 3 de la loi de 2018 sur le retrait de l'Union européenne, telle que modifiée par l'annexe 1 de la loi de 2018 sur la protection des données, la vie privée et les communications électroniques (modifications, etc.) (sortie de l'UE) de 2019 (le « RGPD **britannique** ») ;
- (b) la loi britannique de 2018 sur la protection des données (la « **DPA 2018** ») ; et
- (c) le règlement de 2003 sur la vie privée et les communications électroniques, qui fait partie intégrante du droit anglais, gallois, écossais et nord-irlandais en vertu de l'article 3 de la loi de 2018 sur le retrait de l'Union européenne, telle que modifiée par le règlement de 2019 sur la protection des données, la vie privée et les communications électroniques (modifications, etc.) (sortie de l'UE) de 2020 (« **PECR** »).

2.3 Sauf indication contraire dans le contexte, les termes « responsable du traitement », « **personne concernée** », « **données à caractère personnel** », « **violation de données à caractère personnel** », « sous-traitant », « traitement » et « **catégories particulières de données à caractère personnel** » doivent être interprétés et compris en référence à la législation sur la protection des données, et les termes « traiter » et « traitement » ont des significations correspondantes.

3 CONFORMITÉ EN MATIÈRE DE PROTECTION DES DONNÉES

3.1 Les parties reconnaissent que, en ce qui concerne les données à caractère personnel du client, le client (ou la filiale concernée du client) est le responsable du traitement et Keyloop est le sous-traitant.

3.2 Keyloop traitera les données à caractère personnel du client conformément aux dispositions relatives au traitement des données.

4 OBLIGATIONS DU CLIENT

4.1 Le client doit, et doit veiller à ce que ses affiliés :

4.1.1 s'assurer qu'il dispose, conformément à la législation sur la protection des données, (i) d'une base légale appropriée ; (ii) de tous les droits et consentements nécessaires de la part des personnes concernées ; et (iii) de toutes les notifications appropriées afin de :

4.1.1.1 divulguer les données personnelles du client à Keyloop ; et

4.1.1.2 permettre à Keyloop de traiter les données personnelles du client comme indiqué dans le contrat, conformément à la législation sur la protection des données ;

4.1.2 fournir rapidement une assistance pour répondre à toute demande de renseignements, enquête ou évaluation du traitement en vertu du présent addendum sur le traitement des données initiée par une autorité de protection des données ;

4.1.3 fournir à Keyloop des instructions écrites documentées, telles que définies dans le Contrat, concernant le traitement des Données personnelles du client ;

4.1.4 être responsable de répondre et de mettre en œuvre les mesures appropriées pour traiter les demandes d'exercice des droits des personnes concernées et les demandes d'accès des personnes concernées, conformément à la législation sur la protection des données ;

4.1.5 réaliser toutes les analyses d'impact relatives à la protection des données lorsque cela est requis par la législation sur la protection des données ; et

4.1.6 remplir à tout moment ses obligations en vertu du présent addendum relatif au traitement des données de manière à ne pas entraîner de violation de la législation sur la protection des données par Keyloop.

5 OBLIGATIONS DE KEYLOOP

5.1 Keyloop doit :

5.1.1 et prendra toutes les mesures raisonnables pour s'assurer que son personnel traite les données personnelles du client uniquement dans le but limité d'exécuter le contrat et conformément aux instructions écrites et documentées du client telles que définies dans le contrat, sauf si la loi applicable en dispose autrement. Dans ce cas, Keyloop informera le Client de cette exigence légale avant le traitement, sauf si la loi applicable l'interdit. Si Keyloop a connaissance ou estime qu'une instruction donnée par le Client enfreint la législation sur la protection des données, Keyloop en informera le Client sans délai injustifié, lorsque la loi applicable le permet.

- 5.1.2 veiller à ce que le personnel autorisé à traiter les données personnelles des clients soit soumis à des obligations de confidentialité applicables par Keyloop ou le sous-traitant concerné ;
- 5.1.3 compte tenu de l'état de la technique, des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques encourus par les personnes concernées, mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté à la protection des données personnelles des clients, notamment contre la destruction accidentelle ou illicite, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé. Les mesures techniques et organisationnelles appropriées mises en œuvre par Keyloop sont répertoriées dans le Centre de confidentialité ;
- 5.1.4 dans la mesure où cela n'est pas possible grâce aux fonctionnalités des Produits et d'une manière compatible avec le rôle de Keyloop en tant que sous-traitant, aider le Client à répondre aux demandes des personnes concernées relatives à leurs droits, à se conformer aux obligations du Client en matière de sécurité, de notification des violations aux personnes concernées et à l'Autorité de protection des données, d'analyses d'impact sur la protection des données et de toute consultation avec l'Autorité de protection des données. En outre, Keyloop informera rapidement le Client :
 - 5.1.4.1 si elle reçoit une demande d'accès de la part d'une personne concernée, ou une demande de transfert, de rectification, d'effacement, de destruction ou de limitation des données personnelles du client ; et
 - 5.1.4.2 de toute demande de divulgation des données personnelles du client émanant d'un tiers et reçue directement par Keyloop, et fournir une copie de cette demande.
- Keyloop ne divulguera ni ne communiquera aucune donnée personnelle du client à d'autres personnes que le client, sauf si la loi applicable l'exige ou le permet ;
- 5.1.5 à la demande du client, restituer les données personnelles du client à celui-ci dans un format qui préserve l'intégrité des données personnelles du client ou détruire ou anonymiser de manière sécurisée les données personnelles du client (y compris toutes leurs copies), sauf si la loi applicable exige que Keyloop continue à stocker les données personnelles du client, auquel cas Keyloop traitera ces données personnelles du client en tant que responsable du traitement. Sous réserve de la clause 14.2 du Contrat, à la résiliation du Contrat, le Client et Keyloop supprimeront et effaceront les données conformément aux clauses 21.2.4 et 21.2.5 des Conditions générales standard ;
- 5.1.6 sur demande (mais pas plus d'une fois par an), fournir au Client une copie d'un audit de la conformité de Keyloop à la législation sur la protection des données (ou à certains aspects de celle-ci). Si le Client estime, de manière raisonnable, que ce rapport est insuffisant pour prouver la conformité de Keyloop, Keyloop permettra au Client (ou à ses représentants autorisés

) un accès raisonnable, pendant les heures de travail normales de Keyloop et à une heure convenue, à tous les locaux et documents pertinents afin d'inspecter les procédures et mesures mentionnées dans le présent addendum sur le traitement des données. Le client ne doit pas perturber les activités habituelles de Keyloop, il ne peut accéder qu'aux ressources qui concernent spécifiquement ses données personnelles et lui (ou son représentant) doit signer un accord de non-divulgaration avant d'être autorisé à y accéder ; et

5.1.7 faire tout son possible pour informer le client dans les 24 heures, et en tout état de cause sans retard injustifié, après avoir pris connaissance d'une violation des données à caractère personnel concernant les données à caractère personnel du client qui sont traitées par Keyloop ou pour le compte de Keyloop dans le cadre du contrat.

5.2 Keyloop se réserve le droit d'appliquer des frais supplémentaires calculés aux tarifs standard pour fournir l'assistance et les informations décrites aux clauses 5.1.4 et 5.1.6.

6 NOMINATION DE SOUS-TRAITANTS

6.1 En concluant le Contrat, le Client autorise Keyloop à nommer les Sous-traitants secondaires répertoriés dans le Centre de confidentialité.

6.2 Le client consent à la modification par Keyloop des sous-traitants lorsque les conditions prévues aux clauses 6.3 à 6.5 sont remplies.

6.3 Keyloop mettra à jour le Centre de confidentialité afin de refléter les détails de chaque sous-traitant au moins 30 jours avant que ce sous-traitant ne traite les données personnelles du client. Le client peut s'opposer à cette modification dans le délai susmentionné s'il estime, de manière raisonnable, que le sous-traitant ne dispose pas des mesures techniques et organisationnelles ou des garanties appropriées requises par le présent addendum relatif au traitement des données ou que la désignation du sous-traitant entraînera un défaut de prestation des services.

6.4 Keyloop informera le Client si le Centre de confidentialité est mis à jour conformément à la clause 6.3.

6.5 Keyloop mettra en place avec tout sous-traitant des obligations contractuelles écrites qui sont :

6.5.1 au moins équivalentes aux obligations imposées à Keyloop conformément au présent addendum relatif au traitement des données ; et

6.5.2 conforme à la législation sur la protection des données.

6.6 Entre Keyloop et le client, Keyloop reste responsable de tout manquement d'un sous-traitant à ces obligations équivalentes en matière de protection des données.

7 TRANSFERTS TRANSFRONTALIERS

- 7.1 Sous réserve du respect de la clause 7.2, Keyloop (et ses sous-traitants) peut transférer les données personnelles du client à des destinataires situés à l'intérieur ou à l'extérieur du territoire, y compris à l'intérieur ou à l'extérieur de l'Espace économique européen (EEE), du Royaume-Uni (RU), de la Suisse ou de tout territoire jugé adéquat par la Commission européenne, le gouvernement britannique ou le gouvernement suisse (selon le cas).
- 7.2 Keyloop effectuera le transfert conformément à la législation sur la protection des données. Ces garanties peuvent inclure le recours à une décision d'adéquation prise par une autorité de protection des données ou dans le cadre d'un contrat comprenant des clauses types obligeant le sous-traitant dans le territoire concerné à mettre en œuvre les dispositions, mesures, contrôles et exigences énoncés dans la législation applicable en matière de protection des données et/ou à réaliser une évaluation du transfert de données comme l'exige la législation sur la protection des données.

ANNEXE 1

Conditions spécifiques au territoire

1. Afrique du Sud

1.1. Toute référence au « responsable du traitement » dans l'addendum relatif au traitement des données inclut dans son champ d'application le terme « partie responsable », toute référence à un « sous-traitant » inclut dans son champ d'application le terme « opérateur » et toute référence au terme « données à caractère personnel » inclut dans son champ d'application le terme « informations à caractère personnel », ces termes étant définis comme suit :

1.1.1. « partie responsable » désigne un organisme public ou privé ou toute autre personne qui, seule ou conjointement avec d'autres, détermine la finalité et les moyens du traitement des informations personnelles ;

1.1.2. « opérateur » désigne une personne qui traite des informations personnelles pour le compte d'une partie responsable dans le cadre d'un contrat ou d'un mandat, sans être placée sous l'autorité directe de cette partie ; et

1.1.3. « informations personnelles » désigne les informations relatives à une personne physique identifiable et vivante et, le cas échéant, à une personne morale identifiable et existante.